UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	MISC NO. GJ3793 **ORAL ARGUMENT REQUESTED**

Unsealed 2/7

MOTION OF REAL PARTIES IN INTEREST JACOB APPELBAUM, BIRGITTA JONSDOTTIR, AND ROP GONGGRIJP TO VACATE DECEMBER 14, 2010 ORDER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Other Authorities

I. INTRODUCTION

Real parties in interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp (collectively "Parties") hereby move to vacate the Court's December 14, 2010 Order requiring Twitter, Inc. to disclose extensive information related to their private Twitter accounts pursuant to section 2703(d) of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("December 14 Order" or "Order"). There is no reasonable basis for the Order and the Court should vacate it for the following reasons.

First, the face of the December 14 Order demonstrates that the government's *ex parte* Application purportedly "showing that there are reasonable grounds" for the Order likely contains material errors or omissions that render the Application insufficient.[1] The face of the December 14 Order indicates that the government's underlying investigation presumably relates, in some way, to the website WikiLeaks. Under 18 U.S.C. § 2703(d), therefore, any application must provide "specific and articulable facts" showing that the Parties' Twitter information sought is both "relevant" and "material" to an on-going investigation about WikiLeaks. No such "specific and articulable facts" could have been provided here, however, because the government has sought information about all of the Parties' Twitter-related publications and speech over a 6 ½ month period of time and all of the Parties' Twitter-based direct messages between themselves and certain others, even though the vast majority of that information has nothing to do with WikiLeaks at all. As such, non-WikiLeaks-related information cannot be relevant or material to a WikiLeaks-related investigation and the government's Application cannot have provided the specific facts needed to justify a proper § 2703 order.

Second, the Order intrudes upon important First Amendment rights. It is impermissibly overbroad because it demands production of information that will not directly further the government's purported interests. Moreover, to the extent that the Parties' Twitter accounts are subject to government snooping because of what the Parties have said and because of who they

[1] As detailed further below, the government's refusal to provide the Parties with its Application, therefore denying the Parties an opportunity to respond directly to its assertions, does not prevent the Parties from challenging these problems because courts have long recognized the right to challenge third-party production demands—even where the request is cloaked in secrecy. In light of this secrecy, the Parties have filed a companion Motion to Unseal the Application. If the Court orders disclosure of such materials, the Parties will supplement this Motion.

know, that it impermissable. They each spoke on Twitter about what has become a political cause, *i.e.*, the WikiLeaks website and its founder Julian Assange. But, the First Amendment guarantees their right to speak up for and freely associate with even unpopular people and causes. Where a disclosure demand implicates First Amendment freedoms, it must be scrutinized with special care and governmental fishing expeditions that improperly intimidate and silence cannot survive First Amendment scrutiny.

Third, the Order threatens the Parties' Fourth Amendment rights because disclosure could reveal that the Parties were located in particular private spaces at particular times—information in which they maintain a reasonable expectation of privacy. The government cannot track movements and location that may reveal intimate details of a person's life without the safeguards of a valid warrant based on probable cause.

Fourth, because the Order and Application raise serious constitutional concerns, the Court should exercise its discretion under § 2703(d) to require the government to obtain a warrant based on probable cause. The Court should exercise this discretion here to avoid the constitutional questions raised by warrantless disclosure and ensure that the Parties' rights are not improperly trampled.

Finally, the demand for information about Ms. Jonsdottir—a Member of the Icelandic Parliament—is contrary to Icelandic law and creates a disturbing precedent regarding a foreign government's ability to collect private data from another country's officials.

When Congress amended the Stored Communications Act in 1994, it emphasized the need to "guard against 'fishing expeditions' by law enforcement." *See* H.R. Rep. No. 103-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.A.A.N. 3489, 3511-12. Here, the Court should do just that by vacating the December 14 Order and denying the government's Application for records related to the Twitter accounts associated with "rop_g"; "ioerror," and "birgittaj."

II. BACKGROUND

On December 14, 2010, this Court entered a sealed order directing Twitter, Inc. to provide the government with records and other information related to the accounts of several of

its users, including the Parties here. Sears Decl.,[2] Exh. 1 (the "Dec. 14 Order'). On January 5, 2011, the Court unsealed the Order. Sears Decl., Exh. 2. Twitter informed the Parties of the record demand two days later. *See, e.g.*, Sears Decl., Exh. 3.

The Parties' Motion for Unsealing of Sealed Court Records, filed concurrently, provides a detailed factual and procedural background. The Parties incorporate that discussion by reference rather than repeat it here. *See* Motion for Unsealing of Sealed Court Records at 4-6.

In sum, the December 14 Order requires Twitter to provide the government with records related to the Parties' Twitter accounts —including home addresses, connection records, and Internet Protocol addresses.[3] *See* Exh. 1 (Dec. 14 Order at Attach. A). Twitter is an on-line communications tool that permits users to express their thoughts in individual messages ("Tweets") of 140 characters or less. *See* Motion to Unseal at 4-6; *see also* http://twitter.com/about. The heart of the service is short, public text messages that express opinions, relate thoughts, and provide commentary. Users can also provide links to other websites (if space permits), "re-tweet" (i.e., re-publish) Twitter messages made by others, and send direct messages to other users.

Here, all three Parties—Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp—have public Twitter feeds they use to express opinion and share commentary on public events and issues. Anyone can read their Tweets at the Twitter website and anyone can sign up to follow the Parties' Twitter feeds. Each of the Parties uses Twitter extensively and/or has thousands of "followers" who follow what they post.

On its face the Dec. 14 Order seeks information about all of those who received the Parties' publications and private messages, mapping their associations and audience. Even after the actual information to be produced under the Order was narrowed by the government pursuant to concerns raised by Twitter,[4] it requires Twitter to disclose such information for all of the

---

[2] Declaration of Stuart Sears In Support of Motion Of Real Parties In Interest Jacob Appelbaum, Birgitta Jonsdottir, and Rop Gonggrijp to Vacate December 14. 2010 Order (hereinafter "Sears Decl.").

[3] An Internet Protocol ("IP") address is a unique numerical address that identifies individual computers or other devices as they interact over the Internet. *See infra* at III.C.

[4] The government has not conceded that its original Order was improper in any manner. Nor has the government agreed never to ask for the full scope of the originally demanded information.

Parties' Twitter-related speech (called "Tweets") for multiple months, *i.e.*, November 15, 2009 to June 1, 2010, regardless of any connection between the postings and WikiLeaks. Such information is also requested for all of the Parties' Twitter-based direct messages between each other during the same multi-month time period—again, regardless of any connection between the messages and WikiLeaks. The Order's breadth is significant because each of the Parties use Twitter extensively and/or have thousands of "followers" who follow what they post – as of January 25, 2011, Mr. Appelbaum has posted 7,909 Tweets and has 10,699 followers, Ms. Jonsdottir has posted 1211 Tweets and has 5,904 followers, and Mr. Gonggrijp has posted 77 Tweets and has 4223 followers. Mr. Appelbaum, Ms. Jondottir and Mr. Gongrijp have also all published many Twitter messages that are wholly unrelated to WikiLeaks, including tweets which comment on the political situations in Tibet and Tunisia, comment on the Icelandic volcano that blanketed Europe with ash in 2010, or address issues such as the TSA, obscenity and gay marriage laws, and charitable causes. *See* Sears Decl. Exh. 4 (examples of the Parties' non-WikiLeaks related Twitter postings). Thus, the Application and Order must be viewed for what they are—an improper and overbroad fishing expedition.

III. ARGUMENT

A. No "specific and articulable facts" exist to show that the information sought is "relevant and material" to an ongoing criminal investigation.

To obtain an order to disclose customer records under the Stored Communications Act, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe that the ... records or information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). In the December 14 Order, the Court found that it appeared "that the information sought is relevant and material to an ongoing criminal investigation" and granted the disclosure request. The Court, however, was constrained in its consideration at that time because it had before it only the government's Application for the section 2703(d) disclosure order. The Parties believe the government's Application must contain material errors or omissions because there can be no reasonable basis

---

As a result, Movants' challenge to the December 14 Order need not be limited to the narrowed demand.

for finding that the information sought here regarding the Parties' Twitter accounts is both "relevant" and "material" to an ongoing investigation.

Section 2703's "specific and articulable" fact standard requires more than mere suspicion to justify a disclosure order. Even in the context of an investigative stop based on suspected illegality, the government cannot simply rely upon an "inchoate and unparticularized suspicion or hunch," but instead must demonstrate specific facts regarding possible illegal conduct to justify a stop. *See, e.g., Terry v. Ohio*, 392 US 1, 27 (1968); *United States v. Jones*, 242 F.3d 215, 217 (4th Cir. 2001) (finding that the "specific and articulable" standard forbids reliance on suspicions or hunches and therefore rejecting a search based upon an uncorroborated tip); *United States v. Brignoni-Ponce*, 422 US 873, 882, 884-85 (1975) (rejecting a search based upon one factor, the defendant's race, because the reasonableness requirement demands more than "broad and unlimited discretion" and instead requires specific facts demonstrating reasons to believe that potential illegal conduct may be occurring). Here, however, the government is reaching beyond a simple investigative stop and is broadly seeking non-public information regarding the Parties' protected Twitter-based speech and associational contacts. At a minimum, therefore, the government must be required to articulate "specific and articulable facts" that do more than speculate about a nexus between the specific information sought and the potential targets of the government's WikiLeaks-related investigation.

Section 2703 also requires the government to meet its materiality requirement before any order may issue. In a number of contexts, the United States Supreme Court and the Fourth Circuit have emphasized that a showing of materiality requires more than mere theoretical relevance. To establish materiality, the party seeking disclosure must establish through more than mere speculation that the information is, *i.e.*, "vital" or "highly relevant" to the inquiry or "helpful" or "essential" to the party's position. *See, e.g., United States v. Valenzuela-Bernal*, 458 U.S. 858, 867-73 (1982) (access to evidence); *Roviaro v. United States*, 353 U.S. 53, 62-65 (1957) (disclosure of informant's identity); *United States v. Smith*, 780 F.2d 1102, 1109 (4th Cir. 1985) (*en banc*) (standard for overcoming classified information privilege).

Tellingly, the Government refuses to provide its Application to the Parties so that the

Parties may directly challenge the Government's statements seeking to justify the search.[5] But, whatever the Application may claim, it cannot tell the whole story and cannot establish that the information sought in this Order is both "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (emphasis added). Indeed, although the face of the December 14 Order suggests that this investigation relates to WikiLeaks[6], the Order requires Twitter to provide the government with records related to thousands of the Parties' "Tweets" over many months that have nothing whatsoever to do with WikiLeaks. The Parties Tweets about issues such as the political situations in Tibet and Tunisia, a volcano in Iceland, the TSA obscenity and gay marriage laws and charitable cases are not relevant to the government's purported investigative purpose—and they certainly cannot be vital or essential to the government's investigation into WikiLeaks.

Moreover, despite the fact that the Parties' Twitter messages cover a broad range of non-WikiLeaks topics, the government wants private information related to the Parties' accounts, all their Tweets and all their direct messages to each other and certain others during the relevant time period—even information that the Parties do not choose to share with the world. This includes the Internet Protocol address ("IP address") information related to each time the Parties logged into Twitter over a 6 ½ month period of time, the IP address information related to the Parties' direct messages to themselves and certain others, and the date and time information related to all the Parties' log ins and direct messages over this multi-month time period. This Order requires production of this information for all the Parties' Tweets and direct messages during a multi-month time period, without regard to whether the messages relate to WikiLeaks or any other specific subject.

In light of the Order's mandate to produce a broad swath of data that has no connection

[5] The Parties have filed a companion Motion to Unseal the Application and will supplement this Motion if the Court orders disclosure. Even if the Application is not unsealed, it should be disclosed to the Parties under seal so they can fairly challenge the December 14 Order and address the government's statements directly on Reply.

[6] Press reports issued after the Order became public confirm this WikiLeaks connection. *See, e.g., Scott Shane and John F. Burns, U.S. Subpoenas Twitter Over WikiLeaks Supporters,* N.Y. Times, Jan. 9, 2011, at A1 *available at* http://www.nytimes.com/2011/01/09/world/09wiki.html; David Batty, *US Orders Twitter To Hand Over WikiLeaks Members' Private Details, The Guardian, Jan. 8, 2011.*

whatsoever to WikiLeaks and cannot be relevant or material to any investigation, the December 14 Order should be vacated, the Application disclosed, and the Parties afforded a fair opportunity to further challenge the Government's assertions and highlight any material misstatements or omissions in the Application. *See Franks v. Delaware*, 438 U.S. 154, 169 (1978).

B. The Order Should be Vacated Because it Intrudes Upon the Parties' First Amendment Rights.

On its face, the Order threatens the Parties' protected First Amendment rights. The Parties' Twitter-related activities are core protected conduct and speech is entitled to the highest level of First Amendment protection. *See, e.g., Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) ("the constitutional guarantees of free speech and free press do not permit the State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action"); *Hess v. Indiana*, 414 U.S. 105, 108-109 (1973) (the state may not criminalize advocacy of the use of force or law-breaking unless the charged conduct is "intended to produce, and likely to produce, *imminent* disorder") (emphasis in original)).

The Supreme Court's holding in *Virginia v. Black*, 538 U.S.343 (2003), illustrates the sanctity of speech. The Court emphasized that the government may not prohibit "dissemination of social, economic and political doctrine"—even that "which a vast majority of its citizens believes to be false and fraught with evil consequence." *Id.* at 358 (citation omitted). Even distasteful and threatening gatherings and speeches are protected in our democracy. *Brandenburg*, 395 U.S. at 447. As the Court explained in *Brandenburg*, efforts to "punish mere advocacy and to forbid, on pain of criminal punishment, assembly with others merely to advocate the described type of action" violate the First Amendment. *Id.* at 449.

Moreover, freedom of association even with unpopular individuals and groups is an inseparable aspect of Constitutional "liberty." *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460 (1958) ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment which embraces freedom of speech."). Indeed, "[t]he right to associate in order to express one's views is 'inseparable' from the right to speak freely." *Cromer*

v. Brown, 88 F.3d 1315, 1331 (4th Cir. 1994) (citation omitted). As the Fourth Circuit explained, "we have long understood as implicit in the right to engage in activities protected by the First Amendment a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." *Id.* (quoting *Roberts v. U.S. Jaycees*, 468 U.S. 609, 622 (1984)); *see also Shelton v. Tucker*, 364 U.S. 479, 486 (1960) ("the right of free association is a right closely allied to freedom of speech and a right which, like free speech, lies at the foundation of a free society").

Here, the government has declared its disapprobation of WikiLeaks and its desire to prosecute somebody associated with it. Attorney General Holder personally proclaimed that the government will prosecute anyone it can and that the Department of Justice's tough talk "is not saber-rattling." *See* Pete Yost, Assoc. Press, *Holder says Wikileaks under investigation*, http://news.yahoo.com/s/ap/20101129/ap_on_go_ca_st_pe/us_wikileaks_holder (Last visited on Jan. 25, 2011). But, no matter how much the Government dislikes any given speech or advocacy, it cannot use that protected conduct as a pretext for searches or a basis for criminality.[7]

The Government's fishing expedition into information about all the Parties' Twitter postings, and about certain of the Parties' direct messages, over a 6 ½ month time period may chill the Parties' and other individuals' rights to speak freely and associate with others. Such governmental efforts that chill expression must be analyzed with particular scrutiny. *North Carolina Rt. To Life v. Bartlett*, 168 F.3d 705, 715 (4th Cir. 1999). Moreover, where "an investigation ... intrudes into the area of constitutionally protected rights of speech, press, association and petition," the government must "convincingly show a substantial relation between the information sought and a subject of overriding and compelling state interest." *Gibson v. Fla. Legislative Invest. Comm.*, 372 U.S. 539, 546 (1963); *see also In re Grand Jury Subpoenas Duces Tecum.*, 78 F.3d 1307, 1312 (8th Cir. 1996) ("A grand jury subpoena will be

[7] Even where an organization is alleged to have illegitimate aims, the government may not paint all supporters or advocates with a broad brush, ignoring the particulars behind each individual's speech, association, and intent. Rather, the actions of persons accused of improperly supporting such groups "must be judged *strictissimi juri*, for otherwise there is a danger that one in sympathy with the legitimate aims of the organization, but not specifically intending to accomplish them by resort to violence, might be punished for his adherence to lawful and constitutionally protected purposes, because of other unprotected purposes which he does not necessarily share." *Noto v. United States*, 367 U.S. 290, 299-300 (1961).

enforced despite a First Amendment challenge if the government can demonstrate a compelling interest in and a sufficient nexus between the information sought and the subject matter of its investigation."); *In re First Na'l Bank*, 701 F.2d 115, 119 (10th Cir. 1983) ("If the district court determines that enforcement of the subpoena would likely chill associational rights, the Government must show a compelling need"). As the Supreme Court has cautioned, "justifiable governmental goals may not be achieved by unduly broad means having an unnecessary impact on protected rights of speech, press, or association." *Branzburg v. Hayes*, 408 U.S. 665, 680-81 (1972).

Courts have long recognized individuals' right to challenge disclosure demands that implicate First Amendment freedoms and reviewed such demands with special care. *See, e.g., Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 501 n.14 (1975) (individuals must have right to challenge third-party subpoena for their records or unconstitutional intrusions could go unchallenged); *Pollard v. Roberts*, 283 F. Supp. 248, 258-59 (E.D. Ark. 1968) (three-judge court), *aff'd* per curiam, 393 U.S. 14 (1968) (enjoining subpoenas directed at third-party bank because enforcement would violate customer's First Amendment rights of association); *In re First Nat'l Bank*, 701 F.2d at 117-19 (remanding for evidentiary hearing on claims that government's compulsion of information from third parties would violate target's First Amendment right of association); *Local 1814, Int'l Longshoremen's Ass'n v. Waterfront Comm'n of N.Y. Harbor*, 667 F.2d 267, 271, 274 (2d Cir. 1981) (upholding district court's decision to narrow third-party subpoena to limit impairment of targets' First Amendment rights of association).[8]

Here, the government's Application and the Order collide directly with the Parties' First Amendment rights, including by seeking private IP address information and other details for all the Parties' Twitter messages posted over a period of more than six ½ months. The government

[8] The Parties recognize that the Fourth Circuit has wondered aloud in *dicta* about how the First Amendment may affect "the standards governing grand jury investigations." *In re Grand Jury 87-3 Subpoena*, 955 F.2d 229, 232-34 (4th Cir. 1992). But in that case, the real party's First Amendment rights were not implicated, so the Court avoided the substantial relationship test issue. *Id.* at 232-33. It specifically did not decide "the 'First Amendment versus Grand Jury' dilemma" that other courts have resolved by requiring the government to satisfy the substantial relationship test, as discussed above.

cannot claim that all—or even most—of these postings have anything to do with WikiLeaks, its criminal investigation, or matters to be considered by the grand jury. The Application and Order also seek details related to all direct messages between the Parties without any apparent showing that any such messages that might exist are related in any way to WikiLeaks, the government's criminal investigation, or matters to be considered by the grand jury. In light of these significant First Amendment concerns, the Government cannot use the Parties' purported association with WikiLeaks as a sufficient basis for obtaining the Twitter records here.

The Court should vacate its December 14 Order and reconsider in light of these First Amendment principles. Unless the government can show that the information sought would further a compelling interest and that the requests here are the least restrictive way to serve that interest, the government's efforts to seek private data regarding the Parties' Twitter use should be rejected.

C. The Order Should be Vacated Because it Threatens the Parties' Fourth Amendment Rights.

In addition to implicating the Parties' First Amendment rights, the Order threatens to violate Parties' Fourth Amendment rights as well. The Order threatens such rights because it requires the production of the IP addresses used by Parties at particular dates and times when they logged into their Twitter accounts. Such information could reveal when Parties were located in particular private spaces and is information in which the Parties maintain a constitutionally-protected reasonable expectation of privacy.

IP address information, linked to date and time, such as that sought in the December 14 Order, could allow the government to discern the physical location of the Parties at the exact time they were publishing on Twitter. As the Second Circuit explained:

> The Internet is comprised of numerous interconnected communications and computer networks connecting a wide range of end-users to each other. Every end-user's computer that is connected to the Internet is assigned a unique Internet Protocol number (IP address), such as 123.456.78.90, that identifies its location (*i.e.*, a particular computer-to-network connection) and serves as the routing address for email, pictures, requests to view a web page, and other data sent across the Internet from other end-users.

Register. com, Inc. v. Verio, Inc., 356 F. 3d 393, 409-410 (2nd Cir. 2004) (citation omitted). In

many instances, this information can then simply and easily be translated into the physical location of the speaker, based on publicly available information.[9] As one Court observed, "the process by which defendants IP addresses can be matched up with specific geographic designations, using a publicly available database operated by the American Registry for Internet Numbers. These geographic designations indicate the 'likely' locations of the residences or other venues where defendants used their Internet-connected computers." *Sony Music Entertainment Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 567 (S.D.N.Y. 2004). To the extent that an IP address alone does not reveal physical location, an IP address in combination with the records of the Internal Service Provider that assigned the IP address to a particular subscriber can still reveal physical location, as explained in the Justice Department's computer search and surveillance manual:

> In a common computer search scenario, investigators learn of online criminal conduct. Using records obtained from a victim or from a service provider, investigators determine the Internet Protocol ("IP") address used to commit the crime. Using a subpoena or other process...investigators then compel the Internet Service Provider ("ISP") that has control over that IP address to identify which of its customers was assigned that IP address at the relevant time....

Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations, ch. II, § (C)(1)(a) at 65, available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (last visited Jan. 24, 2011). Thus, by demanding the IP addresses linked to each date and time that each of the Parties logged into the Twitter service over a multi-month period, the government can use such information to try to determine the Parties' locations at the very times they were engaged in publishing—regardless of whether the underlying speech was related to WikiLeaks, and regardless of whether they were Tweeting from a public or a private space.

The government's request for IP addresses here is significant given how such information

[9] The accuracy of IP Address geolocation can depend on many factors, including how an ISP has set up its network of servers and whether an Internet user utilizes one of several tools that allow Internet users to obfuscate their IP addresses. However, one of the leading companies advertises that its free gelolocation tool can determine the location of "79% [of U.S. IP addresses] within a 25 mile radius." MaxMind web site, <http://www.maxmind.com/app/geolitecity> (accessed November 19, 2010).

may reveal location information. Over a quarter of a century ago, the Supreme Court held in *United States v. Karo*, 468 US 705 (1984), that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. In *Karo*, the police placed a primitive tracking device known as a beeper inside a can of ether and used it to infer that the ether remained inside a private residence. In considering the Fourth Amendment challenge to the use of the beeper, the Court held that using an electronic device to infer facts about "location[s] not open to visual surveillance," such as whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Karo*, 468 U.S. at 714-15. Such location tracking, the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, whether it reveals that information directly or enables inferences about the contents of protected spaces. *Id.* at 707, *see also Kyllo v. United States*, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home."). This reasonable expectation of privacy in the contents of protected spaces is not limited to the home but extends to other private spaces as well.[10] *See, e.g., See v. City of Seattle*, 387 US 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483 486 (1964) (hotel room).

[10] Although the Parties have not found any cases specifically addressing Twitter data, numerous courts have recognized that computer users also have a reasonable expectation of privacy in their computer-related data. *See Trulock v. Fresh*, 275 F.3d 391, 402-403 (4th Cir. 2001) (determining whether a search of computers was reasonable under 4th Amendment standards and holding that the plaintiff "had a reasonable expectation of privacy in the password protected computer files"); *United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010) (reviewing computer searches under 4th Amendment standards and cautioning that those "involved in searches of digital media need to exercise caution to ensure that...searches are narrowly tailored to uncover on those things described" in a warrant); *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (noting 4th Amendment concerns in searching computer stored data, particularly where relevant and non-relevant files are "intermingled" together); *see also United States v. Warshak*, 2010 WL 5071766 at ** 11, 14 (6th Cir. Dec. 14, 2010) (noting that given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment Protection" and therefore holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are shared with, or sent or received through, a commercial ISP'").

Relying on *Karo* and *Kyllo*, the Third Circuit recently concluded that the records of a cell phone provider that indicate the location of a subscriber's cell phone ("cell site location information" or "CSLI") may violate the Fourth Amendment to the extent such records can establish that a cell phone was in a particular private space at a particular time. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010) ("*Third Circuit Opinion*"). Specifically, a majority of the Panel concluded that it "cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject" and is therefore protected under *Karo*. *Third Circuit Opinion*, 620 F.3d at 312; *see also id.* at 320 (Tashima, J., concurring) (citing *Kyllo* for the proposition that government access to CSLI absent a showing of probable cause would violate the Fourth Amendment if that information "reveals a cell phone user's location within the interior or curtilage of his home").

Importantly, the Third Circuit held that a cell phone user's Fourth Amendment interest in CSLI is not eliminated by the fact that such information is a record of the phone company. Distinguishing the telephone dialing information that the Supreme Court found to be unprotected under the Fourth Amendment in *Smith v. Maryland*, 442 U.S. 735, 744-45 (1979), the Court emphasized that cell phone users do not voluntarily convey their location to the phone company. When a cell phone user makes a call, the only information voluntarily and knowingly conveyed to the phone company is the number that is dialed—there is no indication to the user that making that call will also locate the caller, let alone generate a permanent record of this location. When a cell phone user receives a call, he has not voluntarily exposed anything at all. *See Third Circuit Opinion*, 620 F.3d at 317 (It is "unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information[,]" therefore "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way.").

The same logic applies to the Parties' records here. Even though records are held by

Twitter, like with CSLI, Twitter users do not voluntarily convey their IP address to the Twitter internet site they visit in a manner that is analogous to the dialing of a telephone. Similarly, as with CSLI, it is unlikely that typical Internet users have any awareness of their IP address, or the fact that it is transmitted to the Internet sites that they communicate with such as Twitter.

The conclusion that IP address information is protected by the Fourth Amendment is further bolstered by the D.C. Circuit's recent conclusion that warrantless use of a GPS device to track the movements of an individual's car over the course of a month violates Fourth Amendment protections. *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), *pet. for reh'g en banc denied* (D.C. Cir. Nov. 19, 2010). As that court explained, even though the car might move in public spaces, "the whole of one's movements over the course of a month is not constructively exposed to the public" and "prolonged GPS monitoring" reveals an intimate picture of the subject's life that he expects no one to have." *Id.* at 561-63. Similarly here, IP address information can reveal an intimate portrait of Parties' movements between the private spaces from which they use the Twitter service.

Thus, the Court, therefore should vacate its December 14 Order and reconsider the government's Application in light of the principles set forth in *Karo*, the *Third Circuit Opinion* and *Maynard*.

D. The Court Should Exercise its Discretion Under 18 U.S.C. § 2703(d) and Avoid Serious Constitutional Questions by Vacating the Order and Requiring a Warrant.

In light of the serious constitutional questions that the Order raises under both the First and Fourth Amendments, if the Court does not vacate the Order completely it should exercise its discretion under § 2703(d) and avoid these constitutional questions by requiring the Government to obtain a warrant based on probable cause.

Although the Stored Communications Act ("SCA") allows the Government to obtain the records sought from Twitter through a court order issued under 18 U.S.C. § 2703(d), the statute also provides courts with the discretion to deny applications for such orders even when the government has made the factual showing required under that section. *Third Circuit Opinion,* 620 4.3d at 315-17. The statute does so by its use of the phrase "only if" in § 2703(d), indicating that the "specific and articulable facts" showing required by that section is a necessary but not

necessarily sufficient condition for a § 2703(d) order. *Id.* The practical effect of such a denial is that the government must instead proceed by obtaining a search warrant based on probable cause, issued under Rule 41 of the Federal Rules of Criminal Procedure pursuant to 18 U.S.C. § 2703(c)(1)(a). *See id.* at 316. Therefore, "the statute as presently written gives the [judge] the option to require a warrant showing probable cause...." *Id.* at 319.[11]

The intent of this "sliding scale" construction of § 2703 is evidenced by Congress' recognition that the Constitution may in some cases protect the privacy of information that would otherwise be available to the Government under § 2703(d). As the Senate Judiciary Committee's report on the statute explained:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information *may* be subject to no constitutional privacy protection.

S. Rep. No. 99-541 at 3 (1986) (emphasis added); *see also, e.g.*, S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] are *not always clear or obvious*.") (emphasis added). In the context of such constitutional uncertainty, it makes sense that Congress would provide a constitutional safety-valve for judges considering government applications under § 2703(d), thereby future-proofing the statute by

---

[11] Ms. Jonsdottir's counsel, EFF and ACLU, served as *amici* to the Third Circuit and the Western District of Pennsylvania on this issue and their briefs provide extensive support for the *Third Circuit Opinion*'s holdings. *See* Brief for Electronic Frontier Foundation, American Civil Liberties Union, ACLU Foundation of Pennsylvania, and Center for Democracy and Technology as Amici Curiae Opposing the Government's Request for Review, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, Magistrate's No. 07-524M, 2008 WL 4191511 (W.D. Pa. 2008), *available at* https://www.eff.org/files/filenode/celltracking/LenihanAmicus.pdf; Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Affirmance, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* https://www.eff.org/files/filenode/celltracking/Filed%20Cell%20Tracking%20Brief.pdf; Brief for Electronic Frontier Foundation et al. as Amici Curiae Opposing Rehearing En Banc, *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010), *available at* https://www.eff.org/files/Filed_Amicus_Opp_to_En_Banc_Petition.pdf

allowing courts the discretion to deny such applications to avoid potential constitutional violations or unnecessary constitutional rulings.

Considering the longstanding doctrine of constitutional avoidance, and particularly in light of the Supreme Court's recent admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies, a Court would properly use its discretion under § 2703(d) when faced with a government application that raises serious constitutional questions. *See City of Ontario v. Quon*, 130 S. Ct. 2619, 2629, 177 L. Ed. 2d 216 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."); *Ashwander v. Tennessee Valley Auth.*, 297 U.S. 288, 347-48 (1936) ("The Court will not pass upon a constitutional question although properly presented by the record, if there is also present some other ground upon which the case may be disposed of.").

As detailed above, the government's Application presents these sort of serious questions—raising serious First and Fourth Amendment concerns. The Court, therefore, should exercise its discretion under § 2703(d), vacate the Dec. 14 Order, and require the government instead to obtain a warrant based on probable cause.

E. The Request for Information about a Member of the Icelandic Parliament, Ms. Jonsdottir, Raises Additional Concerns.

The government's demand for records for Ms. Jonsdottir, an elected member of the Icelandic Parliament, raises additional concerns. Such an investigation appears to violate Icelandic law. As indicated by the attached letter from the Acting Permanent Secretary of State for Iceland, Sears Decl, Exh. 5, and the Decision by the Inter-Parliamentary Union, Sears Decl., Exh. 6, Ms. Jonsdottir is protected by a strong constitutional immunity in Iceland, rooted in Article 49 of the Icelandic Constitution and a similar provision in the Icelandic Law on criminal procedure. Similar immunities exist for Parliamentarians around the world.[12] Ms. Jonsdottir's Tweets are predominantly in Icelandic and largely concern issues arising in Iceland, such as legislation sponsored by Ms. Jonsdottir, the Icelandic debt crisis, and the Icelandic volcanic

[12] The members of the U.S. Congress enjoy similar immunities, rooted in Article I, Section 6, Clause 1, of the U.S. Constitution.

Dated: January 26, 2011

By: _____ with permission for:

Rebecca K. Glenberg, VSB No. 44099
AMERICAN CIVIL LIBERTIES UNION
OF VIRGINIA FOUNDATION, INC.
530 E. Main Street, Suite 310
Richmond, Virginia 23219
Telephone: (804) 644-8080
Facsimile: (804) 649-2733
Email: rglenberg@acluva.org

Cindy A. Cohn (*pro hac vice* pending)
Lee Tien (*pro hac vice* pending)
Kevin S. Bankston (*pro hac vice* pending)
Marcia Hofmann (*pro hac vice* pending)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x108
Facsimile: (415) 436-9993
Email: cindy@eff.org
Email: tien@eff.org
Email: bankston@eff.org
Email: marcia@eff.org

Aden J. Fine (*pro hac vice* pending)
Benjamin Siracusa-Hillman (*pro hac vice* pending)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Telephone: (212) 549-2500
Facsimile: (212) 549-2651
Email: afine@aclu.org
Email: bsiracusahillman@aclu.org

Attorneys for BIRGITTA JONSDOTTIR

eruption. *See* Sears Decl., Exh. 4. Thus, the government's overbroad demand for information about Ms. Jonsdottir creates a situation where the U.S. government is conducting a criminal investigation which sweeps in Ms. Jonsdottir's publications in Icelandic on topics of Icelandic concern—records that could not be obtained under Icelandic law.

Unfortunately this investigation creates a perilous precedent for foreign government efforts to seek information about members of the U.S. Congress. This concern is yet another reason why the Order should be vacated as to Ms. Jonsdottir.

IV. CONCLUSION

For the foregoing reasons the Court should vacate its December 14, 2010 Order requiring Twitter to disclose the Parties' Twitter records related to the Parties and their accounts associated with "rop_g"; "ioerror", and "birgittaj."

Dated: January 26, 2011

By: _____

John K. Zwerling, VSB No. 8201
Stuart Sears, VSB No. 71436
ZWERLING, LEIBIG & MOSELEY, P.C.
108 North Alfred Street
Alexandria, VA 22314
Telephone: (703) 684-8000
Facsimile: (703) 684-9700
Email: JZ@Zwerling.com
Email: Chris@Zwerling.com
Email: Andrea@Zwerling.com
Email: Stuart@Zwerling.com

John W. Keker (*pro hac vice* pending)
Rachael E. Meny (*pro hac vice* pending)
Steven P. Ragland (*pro hac vice* pending)
KEKER & VAN NEST LLP
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188
Email: jkeker@kvn.com
Email: rmeny@kvn.com
Email: sragland@kvn.com

Attorneys for JACOB APPELBAUM

Dated: January 26, 2011

By: /s/ with permission for

Nina J. Ginsberg, VSB No. 19472
DIMUROGINSBERG, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: 703-684-4333
Fax: 703-548-3181
Email: nginsberg@dimuro.com

John D. Cline (*pro hac vice* pending)
LAW OFFICE OF JOHN D. CLINE
115 Sansome Street, Suite 1204
San Francisco, CA 94104
Phone: 415.322.8319
Fax: 415.524.8265
Email: cline@johndclinelaw.com

K.C. Maxwell (*pro hac vice* pending)
LAW OFFICE OF K.C. MAXWELL
115 Sansome Street, Suite 1204
San Francisco, CA 94104
Phone: 415.322.8817
Fax: 415.888.2372
Email: kcm@kcmaxlaw.com

Attorneys for ROP GONGGRIJP

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing pleading was delivered by hand this 26th day of January, 2011, to the U.S. Attorney Box located in the Clerk's office, addressed to:

Tracy Doherty McCormick
U.S. Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
Ph: 703 299-3715
Email: Tracy.McCormick@usdoj.gov

Stuart Alexander Sears